UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,715	07/01/2003	Luz Maria Soto	010942-0304513	3762

27498 7590 06/11/2008

PILLSBURY WINTHROP SHAW PITTMAN LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/612,715	SOTO ET AL.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) *27 and 28* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments and Arguments

1. The Applicant's amendment, filed 29 February 2008, has been received, entered into the record, and respectfully and carefully considered.

2. As a result of the amendment, claims 7 and 20 have been amended. Claims 1-28 are pending in the application and claims 27-28 were previously withdrawn from consideration due to a restriction requirement.

3. Applicant's arguments filed 29 February 2008 have been respectfully and carefully considered. Some of them are persuasive and some of them are not.

4. Applicant's arguments are summarized as below:

a. Withdraw 112 2nd rejection to claims 6 and 19 (Remark pages 8-9)

b. Waugh does not teach, sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user (Remarks pages 9-10)

c. Hale - Brandys never teaches or refers to keys, key generators, key generation, key administrator, pre-enrollment or enrollment and 103 rejection should be withdrawn (Remarks pages 11-12)

d. Dependent claims are allowable due to dependency (Remark page 11).

In response to argument 'a', the examiner withdraws the 112 2nd rejection due to Applicant's amendment and explanation.

In response to argument 'b', the examiner respectfully traverses. It appears that the Applicant is not interpreting the previous action as intended by the examiner. First, the examiner

respectfully asks the Applicant is "sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user" not well known in the art? According to examiner's telephone conversation with Mr. Mark Danielson (Reg. 40,580) on October 25, 2007, Mr. Danielson believes that the novel feature of the instant application is in claims 1 and 14 that wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevent until the user's biometric sample is verified. The examiner updated the search and applied Waugh reference. Waugh reference discloses wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevent until the user's biometric sample is verified. Second, it appears to the examiner that the Applicant indeed argues sending the collected biometric sample from the client to the authentication server via the network. But in claims 1 and 14 of the current application recite, "sending the collected biometric sample from the client to the authentication server" and it does **not** recite "sending the collected biometric sample from the client to the authentication server **via the network**". Third, the examiner respectfully reminds the Applicant that "server" can be interpreted as **software/application** that performs services for connected clients as part of a client-server architecture (Please see examiner's cited Wikipedia.org definition for server listed on PTO -892). Fourth, in col. 3, line 65 - col. 4, line 1, Waugh discloses "The client computer 22 also includes an ID template storage module 42 for storing an ID template downloaded over the network connection 26 from the template server 28". Further, in col. 4, lines 47-64, Waugh teaches, "Referring to Fig. 3, there is illustrated an ID template 80 that is storable in the ID template server 28 and can be downloaded to the ID template storage module 42. The ID template 80 includes a biometric standard storage element 82, a biometric recognition means 84, a,

digital identifier 88 and a release means 86 for releasing the digital identifier 88 when the biometric recognition means 84 about recognizes a biometric value that substantially corresponds to the biometric standard stored in the biometric standard storage element 82. As illustrated in FIG. 3, the biometric standard storage element 82 is linked to the biometric recognition means 84, which, in turn, is linked to the release means 86. The private key is embedded in the digital identifier 88 to enable the private key to be used without being seen or copied. When the digital identifier 88 is released, the key control module 46 decrypts the digital identifier using a control key to obtain the private key. The private key is then sent to the encryption/decryption module." In another words, the ID template, an authentication server is transferred to the ID template storage module in order to recognize a biometric value that substantially corresponds to the biometric standard stored in the biometric standard storage element 82 and finally to release the private key from the digital identifier in the ID template to the encryption/decryption module.

Therefore, Waugh discloses sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user.

In response to argument 'c', the examiner respectfully traverses. The examiner respectfully responds that there are many more portions of the reference cited in the rejection of record, and that in view of the totality of these disclosures these features are well known. First, the Applicant's argument are all focused on the names of keys instead of what they are actually doing since you can come up with a million synonyms for different keys. Second, The examiner begins by considering the scope and meaning of the terms of different keys, which must be given their broadest reasonable interpretation consistent with Applicant's disclosure, as explained in *In re* Morris, 127 F. 3d 1048,

1054 (Fed. Cir. 1997) and see also *In re* Zletz, 893 F. 2d 319, 321 (Fed. Cir. 1989), in which stating the claims must be interpreted as "broadly as their terms reasonably allow". The examiner further states, "the ordinary meaning of a claim term is its meaning to the ordinary artisan after reading the entire patent." *Philips V. AWH Corp., 415 F. 3d 1303, 1321 (Fed. Cir. 2005).* Upon reviewing Applicant's Specification, the examiner fails to find any definition of different keys as claimed by the Applicant – that is different from the ordinary meaning. The examiner finds the ordinary meaning of the term "key" is a parameter or information to identify/verify a user. Hale reference discloses in the abstract "a first memory in the terminal that is assigned to a particular user is initialized by storing therein **a file number associated with the particular user, an assigned terminal number of the terminal, an assigned algorithm**, and **a first number derived from the use in the assigned algorithm of the assigned terminal number** and a secret PIN number entered by the particular user into the terminal**. The file number of the user and the terminal number and algorithm associated with that file number** are also stored in a second memory in the central processor as another part of the initialization procedure. In a subsequent operation, a user enters his secret PIN number and a desired file number into the terminal. **That current secret PIN number and the terminal number are used in the assigned algorithm to compute a second number**. If the first and second numbers properly compare, the user is verified and the terminal transmits the desired file number to the central processor. In response to this desired file number, the central processor causes **a random number to be generated**. The terminal uses this **random number and its assigned terminal number and algorithm to calculate a third number** which is applied to the central processor. At the same time the central processor uses **this random number and the terminal number and algorithm which are both associated with the desired file number to**

calculate a fourth number. If the third and fourth numbers properly compare in the central processor, the terminal is verified and access to the desired file number is allowed", which met the claimed limitation of verification features of generating pre-enrollment keys for the user; supplying the pre-enrollment keys to respective key generators; and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators and verifying registration of the user in accordance with a comparison of the final enrollment key. Furthermore, Brandys discloses in col. 3, lines 42-53, "...this is performed prior to the registration process for biometric information samples" and "...generating subsequent to receiving the biometric information...a private key" in claim 1, which met the claimed limitation of creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user identification information with the final enrollment key

In response to argument 'd', the examiner respectfully traverses. Applicant's argument for claims 1 and 14 as discussed above are traversed and therefore, the Applicant's arguments for dependent claims are based on dependency on claims 1 and 14 are traversed and they are not allowable.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-5, 9-18 and 22-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Waugh et al. (U.S. Patent No. 6,678,821).

As per **claims 1 and 14**, Waugh et al. discloses a method/apparatus ("Method and system for **restricting access to the private key of a user** in a public key infrastructure" – Title) comprising:

storing a private key associated with a user at an authentication server ("(a) storing a plurality of keys; (b)...whether a prospective user of a key in a plurality of keys is the associated user of the key...." – e.g. col. 2, line 65- col. 3, line 3; "one way of conveniently allowing use of both private and public keys is to store such keys on servers – as the ID template server 28 and the certificate authority server 34 respectively...the private keys...from the servers on which these keys are stored" – e.g. col. 4, lines 31-37; "Preferably, for each key in the plurality of keys a biometric standard determined by measuring a selected feature of the associated user is stored in the key storage means" – e.g. col. 2, lines 38-40, "...(a) at least one key storage medium for storing a plurality of keys, each key being useable by an associated user in a public key infrastructure..." – claim 1 and abstract. Please note ID template of the ID template server 28 and the certificate authority sever 34 corresponds to Applicant's an authentication server);

receiving a request for access to a service from the user ("Referring to Fig. 4, there is illustrated a preferred method...of Fig. 1. In step 100, a first user writes or Otherwise generates a message that is to be encrypted and sent to a second user. However, the first user does not know his own private key..." – e.g. col. 4, line 65 - col. 5, line 2 and

"encryption/decryption might be wholly limited to the client computer itself, or to a computer isolated from any network. The browser might then be used to encrypt documents that are stored on the user's computer to preserve confidentiality" – e.g. col. 7, lines 3-7);

collecting a biometric sample from the user associated via a client associated with the user and remote from the authentication server on a network (e.g. col. 5, lines 3-15);

sending the collected biometric sample from the client to the authentication server (e.g. col. 5, lines 3-15, col. 7, lines 3-7, col. 3, line 65 - col. 4, line 1 and col. 4, lines 47-64);

comparing, at the authentication server, the biometric sample to a biometric template associated with the user (step 106 in fig. 4 and col. 4, lines 47-64); and

if a result of the comparing step indicates a match between the biometric sample and template for the user (step 108 in fig. 4):

allowing the private key from the authentication server to be accessed and used with the request (e.g. col. 5, lines 22-30); encrypting the request with the private key (step 108 in fig. 4 and col. 5, lines 31-33), and

providing the service with access to a public key corresponding to the private key, wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template (e.g. step 108 in fig. 4 and col. 5, lines 44-53 and claims 1 and 2).

As per **claims 2-3 and 15-16**, Waugh et al. further discloses if the result indicates a match, generating a digital signature using the private key and for use with the request and

further providing the digital signature to the service associated with the request (e.g. col. 1, lines 52-55, claim 13 and 27)

As per **claims 4 and 17**, Waugh et al. further discloses providing a biometric signature corresponding to the collected biometric sample to the service associated with the request (e.g. col. 5, lines 7-12).

As per **claims 5 and 18**, Waugh et al. further discloses comprising:

allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step (e.g. step 108 in fig. 4. Please note "**if there is**...").

As per **claims 9-11 and 22-24**, Waugh et al. further discloses encrypting the collected biometric sample for transmission to the authentication server; and including integrity information in the encrypted biometric sample and decrypting the encrypted biometric sample at the authentication server; and checking the integrity information included with the biometric sample (e.g. col.5, lines 22-33 and claim 1) and wherein the integrity information includes a unique transaction identifier (e.g. col. 5, lines 3-33 and claim 1. Please note digital identifier corresponds to Applicant's unique transaction identifier).

As per **claims 12 and 25**, Waugh et al. further discloses comprising: associating user identification information with the private key; and maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server (e.g. col. 5, lines3-8 and col. 6, lines 51-56).

As per **claims 13 and 26**, Waugh et al. further discloses wherein the biometric sample includes a fingerprint scan (e.g. col. 5, lines 8-12).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

10. Claims 6-8 and 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waugh et al. (U.S. Patent No. 6,678,821) and further in view of Hale (U.S. Patent No. 4,652,698) and Brandys (U.S. Patent No. 7,188,362).

As per **claims 6-8 and 19-21**, Waugh et al. does not discloses generating pre-enrollment keys for the user; supplying the pre-enrollment keys to respective key generators; and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators, verifying registration of the user in accordance with a comparison of the final enrollment key; creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user identification information with the final enrollment key.

However, the above features are well known in the art. Hale et al. discloses the common user verification features of generating pre-enrollment keys for the user; supplying the pre-enrollment keys to respective key generators; and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators (e.g. abstract) and verifying registration of the user in accordance with a comparison of the final enrollment key (e.g. abstract)

It would been obvious to a person with ordinary skill in the art at the time of the invention to combine Hale et al.'s above user verification features with Waugh et al. motivated by "verify that user is the proper user" (e.g. abstract) to provide "a security system and method" (e.g. abstract).

Waugh et al. – Hale et al. does not disclose creating the biometric template for the user only if registration is verified; and generating the private key only if the biometric template is successfully created associating user identification information with the final enrollment key. However, this well-known feature is disclosed in Brandys (e.g. col. 2, lines 32-38, col. 3, lines 42-53 and claim 1).

It would have been obvious to a person with ordinary skill in the art to combine the well-known features of Brandys' with Waugh et al motivated by "a need for new and improved systems for authenticating messages. The system should analyze biometric information as provided by the user as part of the authentication process. The system should also include features to safeguard the keys that are used in the authentication process.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892)

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2135

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135